UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

34415 7590 02/25/2010

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
KIM, PAUL	
ART UNIT	PAPER NUMBER
2169	

DATE MAILED: 02/25/2010

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,989	08/22/2003	William E. Sobel	20423-08016	8643

TITLE OF INVENTION: SOURCE INDEPENDENT FILE ATTRIBUTE TRACKING

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	05/25/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

34415 7590 02/25/2010

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,989	08/22/2003	William E. Sobel	20423-08016	8643

TITLE OF INVENTION: SOURCE INDEPENDENT FILE ATTRIBUTE TRACKING

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	05/25/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
KIM, PAUL	2169	707-728000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,989	08/22/2003	William E. Sobel	20423-08016	8643

34415 7590 02/25/2010

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
KIM, PAUL	
ART UNIT	PAPER NUMBER
2169	

DATE MAILED: 02/25/2010

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 232 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 232 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	10/645,989	SOBEL, WILLIAM E.	
	Examiner	Art Unit	
	PAUL KIM	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 13 January 2010*.

2. ☒ The allowed claim(s) is/are *1, 3-5, 7-9,11-13,15-16,18-20, and 24-28*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brian Hoffman on 8 February 2010.

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3. The application has been amended as follows:

1. (Currently Amended) A computer implemented method for gleaning file attributes independently of file format, the method comprising the steps of:

a non-application-specific file attribute manager receiving a plurality of files in a plurality of formats, the plurality of files including a plurality of copies of a selected file from the plurality of files;

the file attribute manager scanning the plurality of received files in the plurality of formats;

the file attribute manager gleaning file attributes from each of the plurality of scanned files based on a communications protocol used to receive each of the plurality of files, the file attribute manager gleaning different file attributes for different communications protocols;

the file attribute manager storing the file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database;

the file attribute manager indexing specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database;

the file attribute manager storing a record for each of the plurality of copies of the selected file, each separate record indexed according to the contents of the selected file from the plurality of files, such that each separate record can be accessed by a single index;

examining one of the plurality of files;

retrieving from the plurality of records in the database a first record associated with the examined one of the plurality of files;

retrieving from the plurality of records in the database a second record associated with a malicious file;

analyzing the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record;

analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and

determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file.

2. (Cancelled)

3. (Previously Presented) The method of claim 1 wherein:

specific types of file attributes are gleaned from a specific file as a function of a format of the specific file.

4. (Previously Presented) The method of claim 1 wherein the file attribute manager indexing specific file attributes indexes according to a secure hash of the contents of each specific file.

5. (Previously Presented) The method of claim 1 wherein the file attribute manager

indexing specific file attributes indexes according to a cyclical redundancy check of the contents of each specific file.

6. (Cancelled)

7. (Original) The method of claim 1 further comprising:

deleting records from the database after the records have been stored for a specific period of time.

8. (Previously Presented) The method of claim 1 wherein the non-application-specific file attribute manager is incorporated into one selected from the group consisting of:

a firewall;

an intrusion detection system;

an intrusion detection system application proxy;

a router;

a switch;

a standalone proxy;

a server;

a gateway;

an anti-virus detection system; and

a client.

9. (Currently Amended) A non-transitory computer-readable storage medium containing a computer program product for gleaning file attributes independently of file format, the computer program product comprising program code for:

receiving a plurality of files in a plurality of formats, the plurality of files including a plurality of copies of a selected file from the plurality of files;

scanning the plurality of received files in the plurality of formats;

gleaning file attributes from each of the plurality of scanned files based on a communications protocol used to receive each of the plurality of files, the file

attribute manager gleaning different file attributes for different communications protocols;

storing the file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database;

indexing specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database;

storing a record for each of the plurality of copies of the selected file, each separate record indexed according to the contents of the selected file from the plurality of files, such that each separate record can be accessed by a single index;

examining one of the plurality of files;

retrieving from the plurality of records in the database a first record associated with the one of the examined plurality of files;

retrieving from the plurality of records in the database a second record associated with a malicious file;

analyzing the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record;

analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and

determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file.

10. (Cancelled)

11. (Previously Presented) The computer program product of claim 9 further comprising:

program code for gleaning specific types of file attributes from a specific file as a function of a format of the specific file.

12. (Previously Presented) The computer program product of claim 9 wherein the program code for indexing file attributes indexes according to a secure hash of the contents of each specific file.

13. (Previously Presented) The computer program product of claim 9 wherein the program code for indexing file attributes indexes according to a cyclical redundancy check of the contents of each specific file.

14. (Cancelled)

15. (Original) The computer program product of claim 9 further comprising:

program code for deleting records from the database after the records have been stored for a specific period of time.

16. (Currently Amended) A computer system for gleaning file attributes independently of file format, the computer system having a non-transitory computer readable storage medium storing computer-executable instructions, the computer-executable instructions comprising:

a reception module, configured to receive a plurality of files in a plurality of formats, the plurality of files including a plurality of copies of a selected file from the plurality of files;

a scanning module, configured to scan the plurality of received files in the plurality of formats, the scanning module communicatively coupled to the reception module;

a gleaning module, configured to glean file attributes from each of the plurality of scanned files based on a communications protocol used to receive each of the plurality of files, the file attribute manager gleaning different file attributes for different communications protocols, the gleaning module communicatively coupled to the scanning module;

a storage module, configured to store file attributes gleaned from each of the plurality of scanned files as a plurality of records in a database, the storage module communicatively coupled to the gleaning module;

an indexing module, configured to index specific file attributes gleaned from specific files according to contents of the specific files, the specific file attributes being stored as ones of the plurality of records in the database, the indexing module communicatively coupled to the storage module;

the storage module, further configured to store a record for each of the plurality of copies of the selected file, each separate record indexed according to the contents of the selected file from the plurality of files, such that each separate record can be accessed by a single index;

an examining module, configured to examine one of the plurality of files, the examining module communicatively coupled to the storage module;

a retrieval module, configured to retrieve from the plurality of records in the database a first record associated with the examined one of the plurality of files, the retrieval module communicatively coupled to the examining module and the storage module;

the retrieval module, also configured to retrieve from the plurality of records in the database a second record associated with a malicious file;

an analysis module, configured to analyze the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record; the analysis module communicatively coupled to the retrieval module;

the analysis module, also configured to analyze one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and

a status module, configured to determine whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file, the status module communicatively coupled to the analysis module.

17. (Cancelled)

18. (Previously Presented) The computer system of claim 16 wherein:
the gleaning module is further configured to glean specific types of file attributes from a specific file as a function of a format of the specific file.

19. (Previously Presented) The computer system of claim 16 wherein the indexing module is further configured to index specific file attributes according to a secure hash of the contents of each specific file.

20. (Previously Presented) The computer system of claim 16 wherein the indexing module is further configured to index specific file attributes according to a cyclical redundancy check of the contents of each specific file.

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Previously Presented) The method of claim 1 further comprising:
responsive to determining the status of the examined one of the plurality of files to be malicious, blocking the examined one of the plurality of files.

25. (Previously Presented) The method of claim 1 further comprising:
responsive to determining the status of the examined one of the plurality of files to be legitimate, not blocking the examined one of the plurality of files.

26. (Previously Presented) The method of claim 1 further comprising:
applying at least one rule specifying how to use the gleaned file attributes to process the examined one of the plurality of files.

27. (Previously Presented) The method of claim 26 further comprising:

selecting the at least one rule from a plurality of rules to apply specifying how to use the gleaned file attributes to process the examined one of the plurality of files.

28. (Previously Presented) The method of claim 1, wherein the plurality of files are received from a network connection.

/Tony Mahmoudi/

Supervisory Patent Examiner, Art Unit 2169